Data Protection Policy

Policy and Finance Committee Approved: 17th May 2023
Due for next Review: 17th May 2026

1. The UK General Data Protection Regulation 2018 (GDPR)

The UK GDPR sits alongside the legal framework established by the Data Protection Act 2018 to balance the needs of organisations to use and collect personal data against the rights of the individual to have personal data kept secure and private.

2. The purposes of the UK GDPR are:

To increase the obligations on organisations when acting as data controllers and processors.
To increase the rights of individuals to ensure that their personal data is respected and only used for legitimate purposes.

3. Definitions:

Personal Data – is any information about a living individual which allows them to be identified from that data such as name, address, email address, photograph.
Data Controller – is the person or organisation who determines how and what data is processed i.e., Fleet Town Council
Data Processor – is the person(s) who handle the data on behalf of the data controller.
Data Subject – is the individual about whom the personal data is processed.
Data Protection Officer – is the individual with responsibility for ensuring data protection compliance.

4. The data controller

Fleet Town council processes personal data relating to staff, visitors, councillors, and others, and therefore is a data controller.
Fleet Town Council is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all staff employed at Fleet Town Council and to external organisations or individuals working on our behalf.

5.1 Data Protection Officer

The data protection officer (DPO) is Rochelle Halliday, Executive Officer, and is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is the first point of contact for individuals whose data Fleet Town Council processes and for the ICO. Our DPO is contactable via the main office number or via email at executive.officer@fleet-tc.gov.uk.

6. Data protection principles

The GDPR is based on data protection principles that Fleet Town Council must comply with. The principles say that personal data must be:

- Processed fairly, lawfully and in a transparent way.
- Collected for specified, explicit and legitimate purposes only.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

Data protection training will form part of induction training of all staff and councillors. Existing staff and council members will have their training updated accordingly.

7. Personal Data Processed

The personal data kept or processed by Fleet Town Council includes but is not confined to the following:

- Names, titles and aliases, photographs, and video images.
- Contact details such as telephone numbers, addresses and email addresses, social media addresses.
- Financial identifiers such as bank account numbers, payment card details for persons hiring facilities, for staff, contractors and for suppliers.
- Demographic and background information on staff and members including gender, age, marital status, employment background and qualifications.
- Some sensitive personal data in relation to staff and members such as racial/ethnic origin, mental and physical health, and trade union affiliation.
- Website data such as IP address and analytical data.

8. Sharing personal data, who with and why.

- Staff personal data is shared with Livepay our third-party payroll our provider.
- Staff personal data is shared with HMRC for PAYE and tax purposes.

- Staff personal data is shared with Legal and General as our pension providers.
- Staff personal data is shared with a Councillor for payroll approval.
- Staff personal data may be shared with our third-party HR support, Sussex HR, and other HR services.
- Recorded CCTV images shared with Hart District Council, Runnymede Borough Council and the Police.
- Staff personal data may be shared, only if required, with HSBC to create accounts for Fleet Town Council purposes.
- Personal data may be shared with other tier Councils when dealing with or passing on correspondence.
- Personal data may be shared with the Councils third part cemetery software provider for the purposes of cemetery administration.
- To contact individuals & organisations.
- To maintain own accounts and records.
- To recruit and employ staff and contractors.

We may also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy safeguarding obligations.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency.

We do not share data outside of the UK.

9. The Legal Basis for Processing Personal Data

There are 3 legal bases for processing personal data:

1. As a public authority, the council has certain powers and duties. Most personal data is processed for compliance with a legal obligation which includes carrying out the council's statutory powers and functions; or
2. In the performance of a contract or during steps to enter into a contract; or
3. With consent. Before using an individual's personal data, the council will obtain that individual's consent.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Fleet Town Council holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested If staff receive a subject access request, they must immediately forward it to the DPO.

10.2 Responding to subject access requests.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.

We will not disclose information if it:

- Likely to cause substantial and unwarranted damage to that individual.
- To prevent automated decisions from being taken in relation that individual.

10.3 Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Likely to cause substantial and unwarranted damage to that individual.
- To prevent automated decisions from being taken in relation that individual.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.

- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. CCTV

Fleet Town Council use CCTV in various locations to provide a safer, more secure environment for its staff, volunteers, and service users and to combat vandalism and theft.

- CCTV is installed for the purpose of staff, public and premise security, and safeguarding.
- The prevention, investigation, and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Monitoring the security of the sites.
- To protect members of the public and private property.

Any enquiries about CCTV please refer to the CCTV policy.

12. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office desks, or anywhere else where there is general access.
- Personal information must not be taken off site.
- Staff and councillors are reminded to change their passwords at regular intervals.
- Staff and councillors are not permitted to store personal information on their personal devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

13. Disposal of records

Personal data that is no longer needed will be disposed of securely through the cross-shredder on site. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records, and overwrite or delete electronic files.

14. Personal data breaches

In the unlikely event of a suspected data breach, we will:

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost.
    - Stolen.
    - Destroyed.
    - Altered.
    - Disclosed or made available where it should not have been.
    - Made available to unauthorised people.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:
    - Loss of control over their data.
    - Discrimination.
    - Identify theft or fraud.
    - Financial loss.
    - Damage to reputation.
    - Loss of confidentiality.
    - Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the staff personal files.
- Where the ICO must be notified, the DPO will do this via the ICO Website (ico.org.uk) or telephone 0303 123 1113 within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored in an access limited folder on the shared drive and a copy will be placed on staff personal file.